SYNCURITY

SYNCHRONIZE YOUR SECURITY OPERATIONS

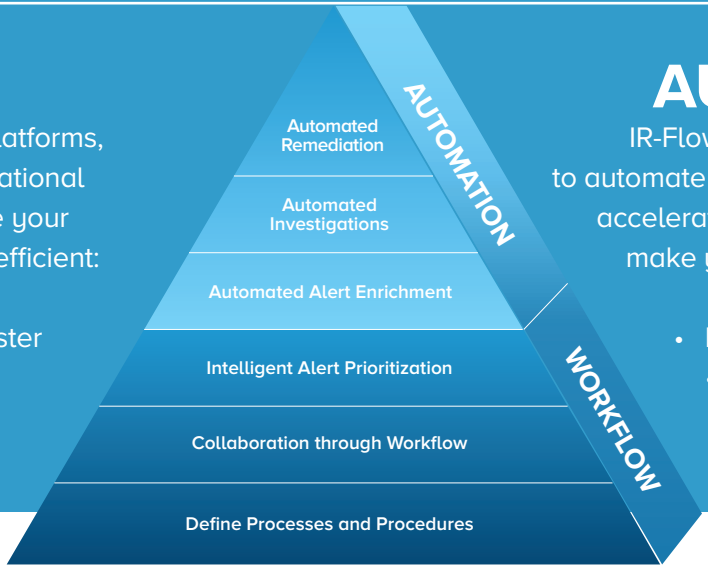
- Implement consistent, repeatable security workflows
- Automate repetitive tasks to improve analyst efficiency
- Enrich alerts automatically to identify true positives faster
- Accelerate alert triage and incident response time
- Deploy pre-built playbooks, checklists and integrations
- Generate customized incident and analyst reports in real time

IR-FLOW: SECURITY OPERATIONS PLATFORM

WORKFLOW

Unlike security automation platforms, IR-Flow first addresses foundational workflow challenges to make your people and processes more efficient:

- Prioritize Critical Alerts Faster
- Codify Incident Response
- Create System of Record



AUTOMATION

IR-Flow then leverages technology to automate manual, repetitive tasks and accelerate incident response steps to make your analysts more effective:

- Integrate Your Security Stack
- Enrich Alerts Automatically
- Streamline Remediation

FORCE MULTIPLY SECURITY TEAMS

Security analysts are overwhelmed with thousands of alerts each day, unable to triage every threat. But automation alone won't eliminate risk. Human validation is necessary to escalate incidents, contain attacks and remediate threats. IR-Flow accelerates triage up to 80 percent, allowing analysts to focus on critical alerts first and take action in minutes not hours.

IMPROVE SECURITY OUTCOMES

CISOs and SOC Managers know that people are their greatest asset. But not all analysts are created equal. Syncurity provides the right balance of workflow and automation to ensure all analysts follow a repeatable, scalable, auditable process. IR-Flow streamlines the entire incident response lifecycle, maximizing ROI and time to value to deliver better security outcomes.

SYNCURITY

SYNCHRONIZING SECURITY OPERATIONS

SIEM Alerts, Emails, APIs

1. Detect

- Integrate Data Sources
- Auto-Enrich Alerts
- Shared Work Queue

MANAGE ALERTS IN A CENTRAL LOCATION

IR-Flow helps analysts move beyond e-mail and spreadsheets by ingesting alerts from SIEMs, security tools, and/or ticketing systems via APIs or email into a unified triage queue. Alerts are automatically enriched with relevant context from security tools without requiring analysts to open multiple browser tabs or run command line queries.

Tier 1 Analyst

2. Triage

- Intelligent Prioritization
- Triage Scoring Engine
- Triage Checklists

PRIORITIZE CRITICAL ALERTS IN SECONDS

Alert handling accounts for more than 80% of all SOC activity. IR-Flow rapidly identifies critical alerts and filters false positives with a patent-pending Triage Scoring Engine®. Analysts validate remaining true positives against pre-defined triage checklists and escalate critical alerts into incidents for investigation.

Tier 2 Analyst

3. Investigate

- Incident Handling
- Custom Playbooks
- Chat & Collaboration

ENFORCE CONSISTENT SECURITY WORKFLOWS

IR-Flow ensures that all analysts implement consistent, repeatable incident response workflows. Quickly codify best practices, policies and procedures into custom playbooks for phishing, malware or ransomware attacks. Syncurity force multiplies your security team, allowing even junior analysts to rapidly adapt to new use cases.

Incident Responder

4. Contain + Remediate

- Case Management
- Threat Intelligence
- Ticketing Systems

RESPOND TO INCIDENTS WITHIN MINUTES

Syncurity allows analysts to manage the entire incident response lifecycle and respond to urgent threats immediately without leaving the IR-Flow interface. Push actions to or pull information from leading threat intelligence, endpoint security and ticketing systems to dramatically reduce time to containment and remediatation.

CISO/SOC Manager

5. Report

- Incident Timelines
- Analyst Performance
- Risk Reduction

ENABLE A NEW LEVEL OF VISIBILITY

Unlike most security automation tools, our workflow engine records all event and activity timestamps, enabling IR-Flow to act as an auditable system of record. CISOs and SOC Managers can focus on optimizing operations, demonstrating improvement, and reducing business risk while simultaneously enabling better security outcomes.

Phone: +1 703 570 4220
E-mail: info@syncurity.net
Website: www.syncurity.net

Syncurity Corporation, 1400 Key Boulevard, Suite 100, Arlington, VA 22209 USA